

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
<b>Stephen A. Thomas</b>	)	Art Unit: <b>2153</b>
	)	
Serial No. <b>10/811,058</b>	)	Confirmation No.: <b>8083</b>
	)	
Filed: <b>March 26, 2004</b>	)	Examiner: <b>Wang, Alex</b>
	)	
For: <b>Intelligent End User Devices For</b>	)	
<b>Clearinghouse Services in An Internet</b>	)	
<b>Telephony System</b>	)	

---

**AMENDMENT AND RESPONSE UNDER 37 C.F.R. § 1.111**

---

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

April 29, 2008

Responsive to the Official Office Action mailed on October 29, 2007 and with a petition and three-month extension of time fee to extend the due date to April 29, 2008, the Applicants submit the following amendments and remarks for the Examiner's consideration.

**AMENDMENT**

**Amendments to the Claims** are reflected in the listing of claims which begin on page 2 of this paper.

**Remarks/Arguments** begin on page 7 of this paper.

---

I hereby certify that this correspondence is being electronically transmitted to: Mail Stop Amendment, Commissioner for Patents, GAU 2153, P.O. Box 1450, Alexandria, VA 22313-1450, Attn: Examiner Wang, on April 29, 2008.

**/SPW/**

---

Steven P. Wigmore Reg. No. 40,447

Claims 1-3. (Cancelled.)

4. (Currently Amended) A computer-implemented method for providing clearinghouse services to a client device in an Internet Protocol (IP) telephony system, comprising the steps of:

transmitting an IP telephony communication session set-up request for an IP telephony communication session to a proxy server from a client application operating on the client device, the client device and the proxy server coupled to an IP network;

transmitting an authorization request from the proxy server to a clearinghouse service running on a service point coupled to the IP network, the clearinghouse service being accessible only by the proxy server and one or more gateways;

generating an authorization response with the clearinghouse service running on the service point;

transmitting an authorization response from the service point to the proxy server via the IP network, the authorization response comprising the identity of one or more terminating gateways coupled to the IP network and available to complete the IP telephony communication session, and an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, the terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token;

selecting one of the terminating gateways with the proxy server to complete the IP telephony communication session;

transmitting via the proxy server the communication session set-up request to the selected terminating gateway via the IP network, the communication session set-up request comprising the electronic authorization token; and

establishing the IP telephony communication session via the selected terminating gateway with the Public Switched Telephone Network (PSTN).

5. (Original) The method of Claim 4, further comprising receiving user authentication information, wherein the user authentication information comprises a pass-word.

6. (Original) The method of Claim 4, further comprising receiving user authentication information, wherein the user authentication information comprises payment information.
7. (Original) The method of Claim 4, further comprising terminating the call set-up request if the client application is not a valid user of the services maintained at the proxy server.
8. (Original) The method of Claim 4, wherein transmitting via the proxy server a communication session set-up request to the selected terminating gateway via the IP network further comprises formatting the set-up request according to one of a H.323 and SIP protocol.
9. (Original) The method of Claim 4, further comprising determining if the proxy server is a valid user of the call delivery services of the selected terminating gateway and determining if an authorization token has been issued by a known and valid clearinghouse service.
10. (Original) The method of Claim 4, further comprising determining if the proxy server is a valid user of the call delivery services of the selected terminating gateway and determining if an authorization token has been issued within an expiration period.
11. (Original) The method of Claim 4, further comprising determining if the proxy server is a valid user of the call delivery services of the selected terminating gateway and comparing a called number and a call identifier to information maintained in an authorization token.

**[The Remainder of This Page Has Been Intentionally Left Blank]**

12. (Currently Amended) A computer-implemented method for providing clearinghouse services to a client device in an Internet Protocol (IP) telephony system, comprising the steps of:

transmitting an IP telephony communication session set-up request to a proxy server from the client device, the client device and the proxy server coupled to an IP network;

transmitting an authorization request from the proxy server to a clearinghouse service running on a service point coupled to the IP network, the service point being inaccessible by the client application;

generating an authorization response with the clearinghouse service running on the service point;

transmitting an authorization response from the service point to the proxy server via the IP network, the authorization response comprising the identity of one or more terminating gateways coupled to the IP network and available to complete the IP telephony communication session[[:]], and an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, the terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token;

launching a client application at the client device and routing the identity of one or more terminating gateways from the proxy server to the client application;

selecting one of the terminating gateways with the client application to establish the IP telephony communication session;

transmitting via the client application, the communication session set-up request to the selected terminating gateway via the IP network, the communication session set-up request comprising the electronic authorization token; and

establishing the IP telephony communication session via the selected terminating gateway with the Public Switched Telephone Network (PSTN).

13. (Original) The method of Claim 12, further comprising terminating the communication session set-up request if the client application is not a valid user of the services maintained at the proxy server.

14. (Original) The method of Claim 12, further comprising determining if the proxy server is a valid user of the clearinghouse services by establishing a secure communications link between the proxy server and the service point and evaluating the proxy server with the service point.

15. (Original) The method of Claim 12, wherein launching a client application at the client device further comprises dynamically constructing a web page.

16. (Original) The method of Claim 12, wherein transmitting via the client application the communication session set-up request to the selected terminating gateway via the IP network further comprises formatting the set-up request according to one of a H.323 and SIP protocol.

17. (Original) The method of Claim 12, further comprising receiving user authentication information, wherein the user authentication information comprises a pass-word.

18. (Original) The method of Claim 12, further comprising receiving user authentication information, wherein the user authentication information comprises payment information.

19. (Original) The method of Claim 18, wherein the payment information comprises a calling card number.

20. (Currently Amended) A system for providing clearinghouse services to a client device, comprising:

- an IP telephony network;
- a proxy server;
- a service point;
- one or more gateways;
- a Public Switched Telephone Network (PSTN); and

a client device for transmitting an IP telephony communication session set-up request to the proxy server from a client application running on the client device, the client device and the proxy server coupled to the IP telephony network; the client device operable for transmitting an authorization request to a clearinghouse service running on the service point, the clearinghouse service being accessible only by the proxy server and the one or more gateways; the service point operable for generating and transmitting an authorization response to the proxy server, the authorization response comprising the identity of one or more terminating gateways coupled to the IP network and available to complete an IP telephony communication session, and an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, the terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token, and completing an IP telephony communication session via the one or more terminating gateways to the Public Switched Telephone Network (PSTN).

21. (Original) The system of Claim 20, wherein the authorization request comprises a called number and a call identifier.

22. (Cancelled.)

23. (Original) The system of Claim 20, wherein the communication session set-up request comprises a called number and user authentication information.

**REMARKS**

The Applicant and the undersigned thank Examiner Wang for his time and consideration given during the telephonic interview of April 10, 2008 and for his careful review of this application. Upon entry of this amendment, Claim 1-3 and 22 have been cancelled and Claims 4-21 and 23 remain pending in this application. The three independent claims are Claims 4, 12, and 20.

Consideration of the present application is respectfully requested in light of the above claim amendments to the application, the telephonic interview, and in view of the following remarks.

**Summary of Telephonic Interview of April 10, 2008**

The Applicant and the undersigned thank Examiner Wang for his time and consideration given during the telephonic interview of April 10, 2008. During this telephonic interview, a proposed amendment to the claims was discussed. The Applicant provided the proposed amendment to the claims in advance of the interview.

The Applicant's representative explained to Examiner Wang that the prior art of record does not provide any teaching of at least the combination of (1) Internet Protocol (IP) telephony communications, (2) electronic authorization tokens generated by the clearinghouse service for each identified terminating gateway, and (3) the terminating gateways operating independently and without direct access by the proxy server (4) such that the proxy server gains access to a terminating gateway only with the electronic authorization token.

Specifically, U.S. Pat. No. 6,615,264 issued in name Stoltz et al. (hereinafter, the "Stoltz reference") was discussed. It was pointed out that the Stoltz reference does not relate in anyway to IP telephony, but rather general computer services. Further, the Stoltz reference does not issue electronic authorization tokens with a clearinghouse service. Instead, the Stoltz reference requires the use of physical tokens, such as smart cards which are inserted into terminals that may request certain services from a computer network.

It was also pointed out that U.S. Pat. No. 6,449,646 issued in the name of Sikora et al. (hereinafter, the "Sikora reference") does not make up for the deficiencies of the Stoltz reference.

Like the Stoltz reference, the Sikora reference does not issue electronic authorization tokens with a clearinghouse service.

After listening to the Applicant's representative, Examiner Wang provided a few suggestions to the claims in order to make them more clear under 35 U.S.C. §112, second paragraph. Specifically, Examiner Wang suggested that the Applicant amend the claims to remove the language "without any control by the proxy server" which previously referred to operations of the terminating gateways in the Applicant's proposed claim amendment. The Applicant's representative agreed to those suggestions and they have been adopted in this paper.

Examiner Wang expressed that he understood the Applicant's representative comments and the concepts presented by the amended claims. Examiner Wang indicated that an update search would be conducted after the Applicant submits the claims in a formal amendment.

The Applicant and the undersigned request Examiner Wang to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202.

#### **Claim Rejections Under 35 U.S.C. §103**

The Examiner rejected Claims 4-23 under 35 U.S.C. § 103(a) as being unpatentable over the Stoltz reference in view of the Sikora reference.

The Applicant respectfully offers remarks to traverse these pending rejections. The Applicant will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

#### **Independent Claim 1**

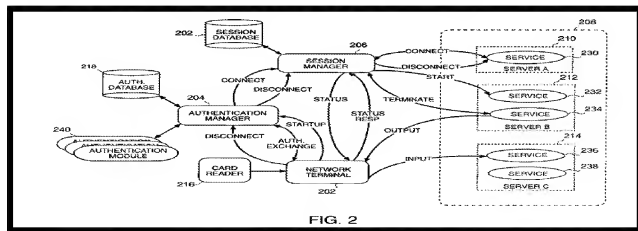
It is respectfully submitted that the Stoltz and Sikora references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) transmitting an IP telephony communication session set-up request to a proxy server from the client device, (2) the client device and the proxy server coupled to an IP network; (3) transmitting an authorization request from the proxy server to a clearinghouse service running on a service point coupled to the IP network, (4) the service point being inaccessible by the client application; (5) generating an authorization response (6) with the clearinghouse service running on the service point; (7) transmitting an authorization response from the service point to the proxy server via the IP



network, (8) the authorization response comprising (9a) the identity of one or more terminating gateways coupled to the IP network and available to complete the IP telephony communication session and (9b) an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, (10) the terminating gateways operating independently and (11) without direct access by the proxy server (12) such that the proxy server gains access to a terminating gateway only with the electronic authorization token; (13) launching a client application at the client device and (14) routing the identity of one or more terminating gateways from the proxy server to the client application; (15) selecting one of the terminating gateways with the client application to establish the IP telephony communication session; (16) transmitting via the client application, the communication session set-up request to the selected terminating gateway via the IP network, (17) the communication session set-up request comprising the electronic authorization token; and (18) establishing the IP telephony communication session via the selected terminating gateway with the Public Switched Telephone Network (PSTN), as recited in amended independent Claim 1.

### The Stoltz Reference

The Stoltz reference describes authentication and session management components and their interactions for providing computer services in the system illustrated in Figure 2 listed below. Network terminal 202 is a human interface device (HID) (e.g., HIDs 821, 822 and 823). An HID has, as examples of its functions, the task of displaying output of services to a user and obtaining input to services from the user. Stoltz reference, column 7, lines 42-48.



Network terminal 202 has the ability to respond to a command (e.g., display command) received from, for example, a software program (e.g., services 230-238, authentication manager 204 and session manager 206) executing on a computational service provider (e.g., computers 710, 711, 712, 713, and 714). The input received from a user is forwarded to, for example, a service that is fulfilling a user request. Stoltz reference column 7, lines 49-55.

More than one server can execute the services that comprise a session. For example, in session 208, service 230 is executing on server 210, services 232 and 234 are executing on server 212 and services 236 and 238 are executing on server 214. A user may access a system (e.g., a server, a session, a service and a network terminal) by initiating a login or other authentication mechanism (e.g., smart card, biometric data, etc.). A separate authentication module 240 may be utilized for each authentication mechanism. During login, the user is validated by an authentication module 240. The authentication modules 240 communicate with authentication manager 240 where a user may be associated with a particular session. Various techniques can be used to allow the user to initiate a login. For example, the user can initiate a login by pressing a key on network terminal 202. Further, a terminal 202 may have screen display icons that allow a user to determine the progress of the authentication process. Stoltz reference column 7, line 56 through column 8, line 6.

A user accesses the system by inserting a smart card in a card reader (e.g., card reader 216) attached to network terminal 202. A smart card is a card that is capable of storing information such as in a magnetic strip or memory of the smart card. The smart card can store user information such as a user's identification (i.e., user ID such as a 64-bit number) and a secret code (e.g., a 128-bit random number) that is transmitted to network terminal 202. The secret code is used during authentication by a smart card authentication module, for example. Stoltz reference column 8, lines 7-16.

Network terminal 202 is aware of (or can obtain) its interconnection network address and the address of authentication manager 204. When a user initiates the login, network terminal 202 initiates communication with authentication manager 204 to begin authentication. Authentication manager 204 is a program active (e.g., executing) on a computational service provider connected to network terminal 202 via an interconnection network such as a local area network (LAN), for example. It should be apparent, however, that network terminal 202 can be connected to authentication manager 204 using other interconnection network technologies such as a fiber

channel loop or point-to-point cables. Network terminal 202 sends a startup request to authentication manager 204 that includes a unique identifier that may correspond to a user. Such an identifier may originate from a token (a particular message or bit pattern that signifies permission to transmit information) or a pseudo token. For example, tokens may be encoded into smart cards and when a smart card is inserted in a card reader at a terminal, the token is transmitted from the terminal 202. Alternatively, a token may be created by a fingerprint reader or other external device. If a smart card is not inserted, or a token is not presented at terminal 202, terminal 202 may construct a "pseudo token" and transmit the pseudo token to authentication manager 204. A pseudo token may be identified by the type associated with it (e.g., "pseudo") and a network interface address such as an ethernet address or a media access controller (MAC) address. Stoltz reference column 8, lines 17-44.

To initiate a connection, a network terminal 202 may be booted up. Once booted, terminal 202 may utilize a dynamic host configuration protocol (DHCP) to obtain application parameters such as the internet protocol address. Terminal 202 then establishes a connection with authentication manager 204 (e.g., using TCP). To establish a connection, terminal 202 may send a message or present a token to the authentication manager 204. Authentication manager 204 then determines whether it wants to take responsibility for this particular terminal/user. In one or more embodiments, authentication manager 204 presents the message (with the token) to one or more authentication modules 240. Stoltz reference column 8, lines 45-57.

In one or more embodiments of the Stoltz system, two authentication modules may be utilized. In such an embodiment, when a token or smart card is inserted at terminal 202, terminal 202 sends a message to authentication manager 204. Authentication manager 204 presents the message to the first authentication module 240. The first authentication module 240 looks up the token in a database to determine if the token is registered with the system. If not (i.e., the first authentication module does not want to accept responsibility for the token/message), the first authentication module passes the token/message onto a second authentication module. The second authentication module may be configured to accept all tokens/messages. Once the token is received, the second authentication module may initiate a registration session and inform the session manager to connect the session to the terminal issuing the request. The registration application presents a form interface to the user where information regarding the user may be obtained (e.g., a username and password or biometric data). Once the information is received, the

information about the user and the token may be stored in a database. Consequently, a token may be bound to a particular user. The registration application may then terminate. Thus, the next time a token is presented to the first authentication module, the token is present and registered with the system so that the first authentication module may take responsibility for the token/message. Using this embodiment, users update a registration database instead of relying on an administrator to manually update information each time a new user is added to a system. Thus, authentication manager 204 is responsible for passing messages onto authentication modules 240, for denying or allowing access to a session, and if allowing access, determining what type of session to present to terminal 202. Stoltz reference column 9, line 46 through column 10, line 12.

#### **What the Stoltz Reference does not Teach**

As noted above in the summary of the telephonic interview, it was pointed out that the Stoltz reference does not relate in anyway to IP telephony, but rather general computer services. Further, the Stoltz reference does not issue electronic authorization tokens with a clearinghouse service. Instead, the Stoltz reference requires the use of physical tokens, such as smart cards which are inserted into terminals that may request certain services from a computer network.

Moreover, the Stoltz reference teaches its authentication manager 204 has direct access to each terminal 202. Meanwhile, the terminating gateways operate independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token;

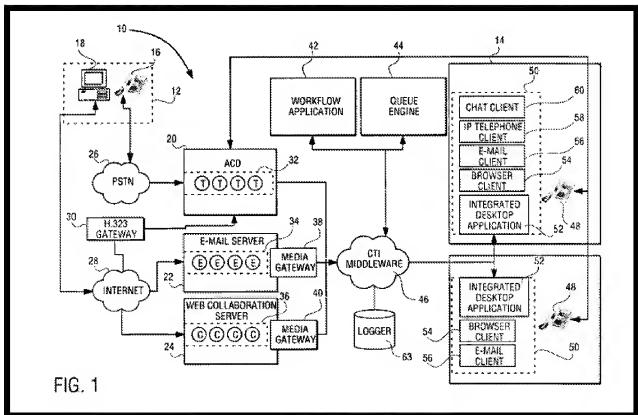
In addition to the Stoltz reference not teaching any electronic authorization tokens, the Examiner also admits that the Stoltz reference fails to provide any teaching of a communication session established by a Public Switched Telephony Network (PSTN).

#### **The Sikora Reference**

To make up for the PSTN deficiency of the Stoltz reference, the Examiner relies upon the Sikora reference. The Sikora reference generally teaches a network-based communications system whereby transactions of a number of varying types, and propagated over a number of varying media types, are allocated to resources capable of processing such transactions.

The Sikora reference teaches a system that can support a telephone call, a facsimile transmission, an electronic mail (e-mail) transmission, a video session, an Internet Protocol (IP) telephone call, a text chat session, a network session or a non-call work event (e.g., case tracking). The system covers transaction processing systems which include Automatic Call Distributors (ACDs), call centers, telephone call processing devices, Private Branch Exchanges (PBXs), web servers, facsimile servers, e-mail servers, switches, routers, and hubs.

A transaction processing environment 10 is illustrated in Figure 1 below which includes a transaction initiator 12 (e.g., a customer) and one or more resources 14 (e.g., human or automated agents) that may be capable of processing and responding to a transaction message generated by the transaction initiator 12. The transaction initiator 12 is shown to have access to a conventional telephone unit 16 and a computer system 18 via which the transaction message may be propagated to a resource 14. The computer system 18 may host any number of application programs for facilitating a transaction. Specifically, the computer system 18 may host a browser application, such as the Netscape Navigator, and an IP telephone application, such as NetMeeting. Sikora reference column 3, lines 39-55.



Additionally, the computer system 18 may host a facsimile transmission/reception application and a telephone call application that allows a customer to send or receive a facsimile and to conduct a regular telephone call utilizing the computer system 18. The transaction initiator 12 may furthermore have access to a stand-alone fax machine or other dedicated e-mail or web devices (not shown in Figure 1). Sikora reference column 3, lines 55-62.

Resources of an exemplary organization are shown to be accessible via three exemplary transaction processing systems, namely an Automatic Call Distributor (ACD) 20, an e-mail server 22, and a web collaboration server 24. Other transaction processing systems, for example, such as a facsimile server or a video server, are not illustrated but may be utilized within the transaction processing environment 10 in a manner similar to that described below with reference to the illustrated transaction processing systems. The telephone unit 16 of the transaction initiator 12 is shown to be coupled to the Public Switched Telephone Network (PSTN) 26 via which a transaction request (e.g., a ring voltage) from the transaction initiator 12 may be transmitted to the ACD 20. Similarly, the computer system 18 is shown to be coupled to the Internet 28, via which a transaction message (e.g., an e-mail message or a text chat request) may be propagated to either the e-mail server 22 or the web collaboration server 24. Further, a voice-over-IP gateway 30 (e.g., a H.323 gateway) is shown to couple the ACD 20 to the Internet 28, to thereby facilitate IP telephone calls between the transaction initiator 12 and a resource 14. Sikora reference column 3, lines 64 through column 4, line 16.

Each of the transaction processing systems 20, 22 and 24 may reside on a dedicated machine, or may each reside concurrently with a further transaction processing system on a shared machine. For example, the email server 22 and the web collaboration server 24 may reside on a single server computer. Each of the transaction processing systems 20, 22 and 24 is furthermore shown to store transaction messages pertaining to, or containing information regarding, respective transactions. For example, the ACD 20 is shown to store a number of telephone call messages 32 (for both switched or IP telephone calls), the e-mail server 22 is shown to store a number of e-mail messages 34, and the web collaboration server 24 is shown to store a number of text chat messages 36. The transaction messages stored on each of the transaction processing systems 20-24 may be stored in queues. For example, the e-mail server 22 may store received e-mail messages in queues according to addressee information, each queue comprising a mailbox designated to a specific e-mail address. The e-mail server 22 and the web

collaboration server 24 are furthermore shown to have respective media gateway applications 38 and 40 associated therewith. Each of the gateway applications 38 and 40 acts as a primary source of interaction between an associated server and downstream intelligence in the form of a workflow application 42 and a queue engine 44. The e-mail gateway application 38 may monitor a Simple Mail Transfer Protocol (SMTP) gateway for incoming e-mail and, responsive to the receipt of an e-mail message at the e-mail server 22, generate a routing message (to be described in further detail below) that is propagated to the workflow application 42. Similarly, the web gateway application 40 monitors the web collaboration server 24 for web requests, and generates a routing message that is propagated to the workflow application 42. Sikora reference column 4, lines 17-50.

The workflow application 42 and the queue engine 44 are coupled to each of the transaction processing systems 20, 22, and 24 via a middleware 46, such as for example of the Prospect Computer Telephony Interface (CTI) System developed by Aspect Telecommunications, Inc. of San Jose, Calif. The media gateway applications 38 and 40 serve to couple the e-mail server 22 and the web collaboration server 24 to the middleware 46, while the ACD 20 may be coupled to the middleware 46 via dedicated software, such as the Application Bridge software developed by Aspect Telecommunications, Inc. The middleware 46 also serves to couple each of the transaction processing systems 20-24, and both the workflow application 42 and the queue engine 44, to each of the resources 14. In the illustrated embodiment, each resource 14 comprises a human agent who has access to a telephone unit 48 and a computer system 50. The computer system 50 is shown to host an integrated desktop application 52, and a number of client programs that interact with the integrated desktop application 52. For example, the computer system 50 may host a browser client 54, an e-mail client 56, an IP telephone client 58 and a text chat client 60. Sikora reference column 4, line 51 through column 5, line 5.

The middleware 46 is also shown to be monitored by a logging application 63 that is responsible for the writing of transaction data to a local Relational Database Management System (RDBMS) (not shown). The logging application 63 is capable of monitoring and logging information regarding any one of a number of transaction types which may be initiated via the transaction processing systems 20-24 and may, for example, record information such as event type, queue time, talk time and termination time by transaction. The logging application 63 may

also generate reports utilizing the record transaction information pertaining to a number of transaction types. Sikora reference column 5, lines 5-16.

#### **What the Sikora Reference Does Not Teach**

Like the Stoltz reference, the Sikora reference also does not issue electronic authorization tokens with a clearinghouse service. The Sikora reference also does not provide any teaching of terminating gateways which operate independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token.

#### **Conclusion Regarding Independent Claim 4**

In light of the differences between Claim 4 and the Stoltz and Sikora references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 4. Accordingly, reconsideration and allowance of amended independent Claim 4 are respectfully requested.

#### **Independent Claim 12**

It is respectfully submitted that the Stoltz and Sikora references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) transmitting an IP telephony communication session set-up request to a proxy server from the client device, (2) the client device and the proxy server coupled to an IP network; (3) transmitting an authorization request from the proxy server to a clearinghouse service running on a service point coupled to the IP network, (3) the service point being inaccessible by the client application; (4) generating an authorization response with the clearinghouse service running on the service point; (5) transmitting an authorization response from the service point to the proxy server via the IP network, (6) the authorization response comprising (7a) the identity of one or more terminating gateways coupled to the IP network and available to complete the IP telephony communication session, and (7b) an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, (8) the terminating gateways operating independently and without direct access by the proxy server (9) such that the proxy server gains access to a



terminating gateway only with the electronic authorization token; (10) launching a client application at the client device and routing the identity of one or more terminating gateways from the proxy server to the client application; (11) selecting one of the terminating gateways with the client application to establish the IP telephony communication session; (12) transmitting via the client application, the communication session set-up request to the selected terminating gateway via the IP network, (13) the communication session set-up request comprising the electronic authorization token; and (14) establishing the IP telephony communication session via the selected terminating gateway with the Public Switched Telephone Network (PSTN), as recited in amended independent Claim 12.

Similar to independent Claim 4, neither the Stoltz nor the Sikora reference provide any teaching of an electronic authorization token generated by the clearinghouse service and terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token.

In light of the differences between Claim 12 and the Stoltz and Sikora references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 12. Accordingly, consideration and allowance of amended independent Claim 12 are respectfully requested.

#### **Independent Claim 20**

It is respectfully submitted that the Stoltz and Sikora references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) an IP telephony network; (2) a proxy server; (3) a service point; (4) one or more gateways; (5) a Public Switched Telephone Network (PSTN); and (6) a client device for transmitting an IP telephony communication session set-up request to the proxy server from a client application running on the client device, (7) the client device and the proxy server coupled to the IP telephony network; (8) the client device operable for transmitting an authorization request to a clearinghouse service running on the service point, (9) the clearinghouse service being accessible only by the proxy server and the one or more gateways; (10) the service point operable for generating and transmitting an authorization response to the proxy server, (11) the authorization response

comprising (12a) the identity of one or more terminating gateways coupled to the IP network and available to complete an IP telephony communication session, and (12b) an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, (13) the terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token, and (14) completing an IP telephony communication session via the one or more terminating gateways to the Public Switched Telephone Network (PSTN), as recited in amended independent Claim 20.

Like independent Claim 4, neither the Stoltz nor the Sikora reference provide any teaching of an electronic authorization token generated by the clearinghouse service for each identified terminating gateway, and the terminating gateways operating independently and without direct access by the proxy server such that the proxy server gains access to a terminating gateway only with the electronic authorization token,

In light of the differences between Claim 20 and the Stoltz and Sikora references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 20. Accordingly, consideration and allowance of amended independent Claim 20 are respectfully requested.

#### **Dependent Claims 5-11, 13-19, 21, and 23**

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 5-11, 13-19, 21, and 23.

#### **CONCLUSION**

The foregoing is submitted as a full and complete response to the Office Action mailed on October 29, 2007. The Applicant and the undersigned thank Examiner Aguirre for consideration of these remarks. The Applicant has amended the claims to overcome the prior art.

The Applicants respectfully submit that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,

/SPW/

Steven P. Wigmore  
Reg. No. 40,447  
April 29, 2008

King & Spalding LLP  
1180 Peachtree Street NE  
Atlanta, Georgia 30309  
K&S File No. 06949-105018